HAL
open science

A secure and smart environment for the transportation of dangerous goods by using Blockchain and IoT devices

Adnan Imeri, Nazim Agoulmine, Djamel Khadraoui

To cite this version:

Adnan Imeri, Nazim Agoulmine, Djamel Khadraoui. A secure and smart environment for the transportation of dangerous goods by using Blockchain and IoT devices. 7th International Workshop on ADVANCEs in ICT Infrastructures and Services (ADVANCE 2019), Jan 2019, Praia, Cape Verde. pp.1–8. hal-02439984

HAL Id: hal-02439984

https://hal.science/hal-02439984v1

Submitted on 14 Jan 2020

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

A secure and smart environment for the transportation of dangerous goods by using Blockchain and IoT devices

Adnan Imeri[1,2], Nazim Agoulmine[2], and Djamel Khadraoui[1]

[1] Luxembourg Institute of Science and Technology
adnan.imeri@list.lu
[2] Universitè of Èvry Val d'Essonne - Paris Saclay University
nazim.agoulmine@univ-evry.fr

Abstract

The impact of the Internet of things (IoT) attributes for a better quality of services in several domains also in transportation. The information generated from IoT devices is essential for daily activity in the domain of transportation. For the transport activities related to dangerous goods, the information shared and exchanged by stakeholders of the supply chain for dangerous goods is considered sensitive and should be protected from the access of unauthorized parties. This paper intends to show the potential of blockchain technology for securing information generated by IoT devices in the context of transportation of dangerous goods.

1 Introduction

In recent years, we witness many changes in the technology domain, which has shaped the current way of performing business processes. The new emerging technologies such as the Internet of Things (IoT) enables redesigning of the new business process. The Internet of Things (IoT) is composed set of devices which are connected for a specific scenario, and they exchange particular information [11]. These devices enable emerging of many technological concepts, such as Smart Manufacturing, Smart City, Smart Home, Smart Offices, etc. [9] [21]. The usability of these technologies, accompanied with particular devices allows better management of enterprise activities, by allowing them to monitor active processes they are performing. The new emerging concepts such as Industry 4.0, intends to transform the way of managing manufacturing, management of logistics and transportation [15]. While the urban activities are growing, there is an implication on increasing services for daily activities. These services may come from the perspective of transportation and other activities which are related to transportation. The use of IoT devices in such environment shows many potentials on better management of service related to transportation, better public information, security, and monitoring for any public activity, thus decreasing challenges in case of accidents. One of the main concerns remains on the privacy and security of information generated by IoT devices [19][33][7]. Through this research paper, we intend to show the potential of blockchain technology for securing the information generated by use of IoT devices in the monitoring the process of transportation of dangerous goods, by approaching a potential real case in Luxembourg.

1.1 Transportation of Dangerous Goods (TDG)

Dangerous goods (DG) are defined as substances which exposes a high risk for humans, living organisms, environment and property. The evaluation of risk exposed by TDG is an challenging task presented by scientific literature [12] [10] [20] [30]. The DG varieties in different classes such as "Explosives", "Gases", "Solids", "Oxidizing materials", "Flammable Liquid", "Radioactive

Figure 1: The map of the route network in Luxembourg. Image Copyright SIP [5]

.

materials, "Corrosive substances", "Miscellaneous" [28]. The DG present a high risk during the transportation process. The challenge originates from the fact that the accidents of anywhere a subject are DG have catastrophically consequence [29]. The significant percentage of TDG is performed every day [27]. A notable presence in transportation statistics is allocated for the TDG, and the transportation network comprises a large number of DG daily [13]. The governance of this process is subject of predefined national and international regulation which determine a sustainable process for TDG. These regulations intend of minimizing the risk by standardizing the process of TDG [17]. The research from [28] elaborates the procedures for packing, labeling, loading, transporting, unloading and warehousing of dangerous goods.

1.2 Challenges regarding TDG in Luxembourg

The TDG involves several challenges because of specificity of the goods which are transporting. The possible accidents with DG demonstrate a high risk for population, private and public properties, and environment since the transportation network usually overpasses urban areas. Following we present the use case of Luxembourg transportation network, that is usually used from other neighbor countries, as a hub for the transportation of goods. Since the most suitable way for TDG is by using roads due to the low costs, compared to other means of transport, the shipping (transport) organization intends to select the shortest route possible to minimize the costs. That exposes a problem, while the transportation network passes through a populated area [27]. This challenge is related to Luxembourg scenario, where main roads move nearby to the populated area, as presented in Figure 1. The highways and local roads, most of the time are massively overloaded with many traffic congestion, and that increases the risk of accidents with DG. For example, the highway (number A31), is massively used by trucks as transit highway for the cross into other neighbor states such as France, Germany, Belgium, and Netherlands.

1.3 The decision support systems as a management tool for TDG

The risk involved in TDG comes from the nature of goods which are subject to transportation. For the risk estimation and management of the processes of TDG, there are designed and develop decision support systems (DSS) as a computer-based solution. The basic idea behind DSS is to help stakeholders to measure the risk for TDG, to save time on critical decision, monitoring the process of transportation [27], decrease the negative impact in case of accidents with dangerous goods [36], scheduling, planning and resource allocation [23][14] [27] [23]. In general, the architecture of these systems is composed of several other systems. The embedded systems for "Sensors", "GPS tracker", "RFID", "GIS for moving objects", and other related ones, which are integrated into the main architecture of DSS, provides information for the process of TDG. The risk analysis, monitoring of the process of TDG and other related tasks are depended on the current state of information which should be provided by these systems. For example, in case of an accident in the process of TDG, the IoT devices (GPS tracker, Sensors, RFID, Raspberry Pi) would provide information regarding this accident in the real time. The information regarding the process of TDG, managed by DSS are stored in the local database of the stakeholders. This exposes several concerns due to the security of information, reliability, and trust issues regarding the process of TDG by other stakeholders or authorities, and we will discuss it on the section below.

1.4 The concern of information security in TDG

The use of IoT devices significantly improves the quality of the process for TDG by advancing the monitoring and reaction in case of abnormal situations, i.e., accidents or other distribution on the process of TDG. The concern of using the IoT devices remains on the security of information exchanged by the IoT devices in the process of TDG [19][33][7]. The current DSS systems are mainly centralized or partly hosted in cloud [7], they remain the only point of reference for data exchange. The IoT frameworks such as Amazon Web Services (AWS) [4], Salesforce [1], does not guarantee the data immutability since they are hosted in the facilities of cloud providers. This way of organizing the storage and management of IoT data does not fulfill the security requirements for the process of TDG.

For the context of TDG, where "nuclear materials or nuclear waste" might be among transporting substance", the security, confidentiality, auditing, and monitoring or processes in real time are extremely recommended. In the line of concerns, the following question raises *"Why we need to secure the information captured from the IoT Devices ?"*.

Since the process of TDG is mostly an international activity, that crosses borders of countries whose stakeholders are involved. For this process, a different international and local regulatory frameworks are applied, and usually, the stakeholders involved are the ones with big market reputation [17]. In case of any accident or irregular process in TDG, the secured information captured from the IoT devices are currently not immutable, and this allows big market players to impact the process by changing the information. The design of current technologies which support the storage of IoT data does not guarantee this level of data security. For ensuring such a system, an extended answer for the following question should be provided:

- Remove the single point of failure in such systems?

- How to secure the information generated by IoT devices?

- How to secure the information provided by stakeholders, e.g., exchange of documents by stakeholders of DG?

- The TDG operations and the process should be auditable?

The primary intention behind this conceptual research is the security of information in the top of DSS or other IoT cloud solutions. For achieving this, we propose a conceptual, described in section 3

2 Related works study: Blockchain and IoT

Blockchain is a distributed database which allows storing of the immutable transaction. The transactions in blockchain might contain financial information, trade information, etc.[32]. The blockchain network is composed of several nodes which communicate with each other in a peer to peer mode. All the nodes included in the blockchain network contain the same ledger, and they relay their communication in each other instead of any central authority [35]. The blockchain nodes gather transaction into "blocks", performs cryptographic check (public-private key cryptography), and seek to add them to the chain of blocks. The process of adding a new block into blockchain is called "mining", and the nodes which perform this mining is called miner. The miner proposes a new block after achieving a consensus challenges set by consensus protocol. The block of transactions which are stored into blockchain are immutable, and cryptography tools ensure data integrity [32]. The fundamental characteristic of blockchain is that the block of data is linked together, so the block N contains the hash address of previous block N-1 [22] [32]. The tendency for changing the information stored into blockchain is denied by consensus protocol e.g., Proof of Work, or Proof of Stake, etc., which verifies the state of data [31].

Smart Contracts: A computer code which is deployed into blockchain and triggered when certain conditions are fulfilled. The smart contracts are self-executed programs for fulfilling given task [2]. An example of smart contract execution is presented for the case of temperature parameters that possibly overcome the fixed level.

IoT devices: RFID, Sensors, GPS tracker, and RaspberyPi, are among IoT devices which are intended to be used for conceptualizing our approach. We will use RFID to store some information about DG. Then, for measurement of temperature, humidity, and abnormal disturbance we will use sensors. GPS tracker devices monitor the location of goods. A more advanced device such as Raspberry will be used to sign transactions.

The scientific community shows many efforts on settling up the new emerging technologies together, blockchain and IoT. A Survey research for the integration of blockchain and IoT is showed in [24], while the challenges and opportunities of integrating blockchain are studied by [25]. A new data transfer layout for IoT based on blockchain technology called IOTA is presented in [3]. The research from [18] presents different architectural styles for using IoT and blockchain. [26] found that the blockchain technology has attractive properties for decentralizing the IoT, thus proposing an architecture for integration blockchain and IoT. The new way of controlling and configuring IoT devices by storing the private key into the device and public key into blockchain nodes [16]. The research from [8] showed that blockchain and smart contract in combination with IoT device, have a significant impact on the automation of processes.

3 Smart and secure environment for TDG

Our conceptual approach intends to change the trend of managing the TDG in line with the security of information. We intend to develop a new way of storing information by using blockchain technology.

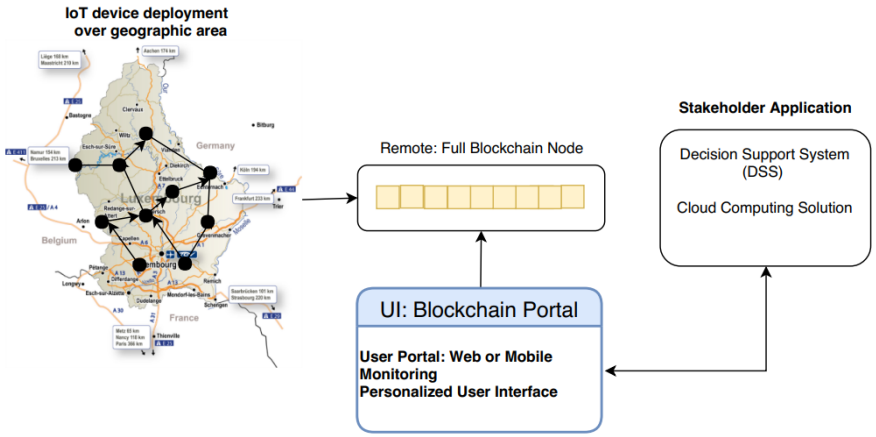

Figure 2: The conceptual approach for smart and secure TDG supply chain

We propose a decentralized solution based on IoT device and blockchain technology. A smart and secure environment in the context of TDG which expect to respond the security concerns presented section 1.4. The sketch from Figure 2, presents the conceptual solution for a smart and secure environment for TDG.

The core of our solution is composed of three main components. The first one represents the IoT devices. The second component is blockchain technology, and the third one is the stakeholder's side, the DSS or any other cloud solution.

For composing the conceptual approach, we deploy the IoT devices over the geographic area and also into transport mechanisms such as trucks. First, these IoT devices are registered on the blockchain, by using their hardware identification [16]. This registration allows them to store their private key in their memory. That avoids receiving information from an unauthorized IoT device. These IoT devices are known as blockchain lightweight node[1], which means that they don't contain complete blockchain, but they use their memory and processing capacity to sign transaction [6]. Second, when the transaction is signed, the IoT device sends this transaction into "Remote Full Blockchain Node", which collect transaction from all IoT nodes and verifies them. There are several mining nodes in our system. For the verification of the transaction, this node checks if the received transactions are from registered IoT device. Further, these nodes add a new block into blockchain. Third, when the block has been added into the blockchain, the *smart contracts* are triggered to fulfill their conditions, in case any parameter is reached, e.g., the high level of temperature on the truck for TDG. Fourth, all stakeholders involved in this process can insert a set of immutable information by using "blockchain portal[2]", for the purpose of the process of TDG, and further, they can monitor the whole process for TDG.

For example, in the context of TDG, the stakeholders initiate this procedure by exchanging information. In our conceptual solution, they can do this by using *"blockchain portal"*. These set of parameter, like the type of goods, itinerary, specific information about DG, e.g., temperature, disturbance, etc., are inserted related to the TDG. Then during the process of transportation, the IoT device detects these goods when reaching its area of detection. The IoT devices receive information regarding the current state of the goods and sign this information by forming a transaction which further will be transmitted into blockchain. The stakeholders and other

[1] The Full Node and Lightweight Node: https://www.mycryptopedia.com/full-node-lightweight-node/
[2] The combination of IPFS and blockchain: https://ipfs.io/

authorized parties can monitor all operations in TDG by using *"blockchain portal"*.
In such an approach, even if some nodes fail to respond, still the system can provide information since the blockchain distributes information in all nodes. The information captured from IoT devices are signed cryptographically and sent to full blockchain nodes making this information immutable. The user interface allows users to provide their data on the blockchain-based system. The ability of immutable record keeping of blockchain enables a full audition of processes and operations for TDG.

4 Technological alignments with business requirements for TDG

The focus behind the proposed conceptual solution for the smart and secure environment for TDG is smart contracts. Various smart contracts are proposed for fulfilling the requirements for the proposed system. Following we detail one of the significant smart contracts:

AlertSC which alerts stakeholders in case of an emergency, i.e., the high temperature of goods. This smart contract is deployed in "Full Blockchain Node" in our solution. It waits without any action until receiving any parameter for triggering it. A simple structure of for this smart contract is expressed below:

```
S0: parameters: stakeholderList, IoTDeviceList, SubstanceList,
     transportedSubstance, location, timestamp, riskLevel, TempLevelSubstance
S1: check (if ReceivedTransaction in IoTDeviceList)
S2: check (if transportedSubstance in SubstanceList) and
            (TempLevelSubstance >=substanceRiskLevel)
S3: check (if stakeholder in stakeholderList)
S4: function (sendMessage: Alert (location, timestamp) -> stakeholder))
```

Along with possibilities offered by the blockchain technology, numerous challenges emerging while aligning business process requirements with the technology features. Mainly the source of these challenges is the insufficient maturity of blockchain technology to respond to all possible business requirements emerged from the business process. The alignment of business requirements rise challenges on the expression of smart contracts. For example, in the context of our study, the legal regulation should be considered in TDG. The expression of legal rules into smart contract arise a research challenges. Further, the performance issue of the blockchain is among the concerns from the scientific community [34]. The main concern in this scenario is the scalability. Regarding this concern in our proposed scenario, while the number of transaction received from IoT devices might be increasing daily in line with transport activity, the current blockchain ability might face difficulty to respond them in real time. Encountering, then the alignment of the business process requirements and the scalability issues we intend to extend our research by implementing the proposed conceptual approach and providing empirical analysis regarding the behavior of the entire system.

5 Conclusion and Future Works

In this paper, we propose a new way of securing information in the process of TDG by combining the IoT devices with blockchain technology. We performed a potential real case scenario, along with it we intend to develop that as proof of concepts in the near future. This approach promises on overcoming of several challenges in the management of process for TDG. Furthermore,

we identified some challenges which stem from combining the IoT devices with blockchain technology. These challenges are on scalability and the alignment of regulatory framework with blockchain technology.

References

[1] Crm software & cloud computing solutions - salesforce emea. https://www.salesforce.com/eu/?ir=1. (Accessed on 11/12/2018).

[2] Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf. http://blockchainlab.com/pdf/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf. (Accessed on 11/14/2018).

[3] iota1_4_3.pdf. https://assets.ctfassets.net/r1dr6vzfxhev/2t4uxvsIqk0EUau6g2sw0g/45eae33637ca92f85dd9f4a3a218e1ec/iota1_4_3.pdf. (Accessed on 11/16/2018).

[4] Machine learning at aws. https://aws.amazon.com/machine-learning/. (Accessed on 11/12/2018).

[5] Road network - luxembourg. http://luxembourg.public.lu/en/cartes-du-luxembourg/05-reseau-routier/index.html. (Accessed on 12/21/2018).

[6] whitepaperanyledger.pdf. http://www.anyledger.io/whitepaperAnyLedger.pdf. (Accessed on 11/13/2018).

[7] Mahmoud Ammar, Giovanni Russello, and Bruno Crispo. Internet of things: A survey on the security of iot frameworks. *Journal of Information Security and Applications*, 38:8–27, 2018.

[8] Konstantinos Christidis and Michael Devetsikiotis. Blockchains and smart contracts for the internet of things. *Ieee Access*, 4:2292–2303, 2016.

[9] Annalisa Cocchia. Smart and digital city: A systematic literature review. In *Smart city*, pages 13–43. Springer, 2014.

[10] Andrea Conca, Chiara Ridella, and Enrico Sapori. A risk assessment for road transportation of dangerous goods: a routing solution. *Transportation Research Procedia*, 14:2890–2899, 2016.

[11] Li Da Xu, Wu He, and Shancang Li. Internet of things in industries: A survey. *IEEE Transactions on industrial informatics*, 10(4):2233–2243, 2014.

[12] Lianhong Ding, Yifan Chen, and Juntao Li. Monitoring dangerous goods in container yard using the internet of things. *Scientific Programming*, 2016, 2016.

[13] Eurostat. Road freight transport by type of goods - statistics explained. https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Road_freight_transport_by_type_of_goods#Road_freight_transport_of_dangerous_goods. (Accessed on 10/29/2018).

[14] William C Frank, Jean-Claude Thill, and Rajan Batta. Spatial decision support system for hazardous material truck routing. *Transportation Research Part C: Emerging Technologies*, 8(1-6):337–359, 2000.

[15] Erik Hofmann and Marco Rüsch. Industry 4.0 and the current status as well as future prospects on logistics. *Computers in Industry*, 89:23–34, 2017.

[16] Seyoung Huh, Sangrae Cho, and Soohyung Kim. Managing iot devices using blockchain platform. In *Advanced Communication Technology (ICACT), 2017 19th International Conference on*, pages 464–467. IEEE, 2017.

[17] Adnan Imeri, Abdelaziz Khadraoui, and Djamel Khadraoui. A conceptual and technical approach for transportation of dangerous goods in compliance with regulatory framework. *Journal of Software*, 12(9):708–722, 2017.

[18] Chun-Feng Liao, Sheng-Wen Bao, Ching-Ju Cheng, and Kung Chen. On design issues and architectural styles for blockchain-driven iot services. In *Consumer Electronics-Taiwan (ICCE-TW),*

2017 IEEE International Conference on, pages 351–352. IEEE, 2017.

[19] Carlo Maria Medaglia and Alexandru Serbanati. An overview of privacy and security issues in the internet of things. In *The Internet of Things*, pages 389–395. Springer, 2010.

[20] Gemma Dolores Molero, Francisco Enrique Santarremigia, Pablo Aragonés-Beltrán, and Juan-Pascual Pastor-Ferrando. Total safety by design: Increased safety and operability of supply chain of inland terminals for containers with dangerous goods. *Safety science*, 100:168–182, 2017.

[21] Taewoo Nam and Theresa A Pardo. Conceptualizing smart city with dimensions of technology, people, and institutions. In *Proceedings of the 12th annual international digital government research conference: digital government innovation in challenging times*, pages 282–291. ACM, 2011.

[22] Michael Nofer, Peter Gomber, Oliver Hinz, and Dirk Schiereck. Blockchain. *Business & Information Systems Engineering*, 59(3):183–187, 2017.

[23] Ebru Vesile Ocalir-Akunal. Decision support systems in transport planning. *Procedia engineering*, 161:1119–1126, 2016.

[24] Alfonso Panarello, Nachiket Tapas, Giovanni Merlino, Francesco Longo, and Antonio Puliafito. Blockchain and iot integration: A systematic survey. *Sensors*, 18(8):2575, 2018.

[25] Ana Reyna, Cristian Martín, Jaime Chen, Enrique Soler, and Manuel Díaz. On blockchain and its integration with iot. challenges and opportunities. *Future Generation Computer Systems*, 2018.

[26] Nabil Rifi, Elie Rachkidi, Nazim Agoulmine, and Nada Chendeb Taher. Towards using blockchain technology for iot data access protection. In *Ubiquitous Wireless Broadband (ICUWB), 2017 IEEE 17th International Conference on*, pages 1–5. IEEE, 2017.

[27] Vincenzo Torretta, Elena Cristina Rada, Marco Schiavon, and Paolo Viotti. Decision support systems for assessing risks involved in transporting hazardous materials: A review. *Safety science*, 92:1–9, 2017.

[28] UNECE. Unece homepage. https://www.unece.org/info/ece-homepage.html. (Accessed on 10/29/2018).

[29] N Vayiokas. Risk assessment of transportation of dangerous goods.

[30] Ningkui Wang, Xiaozhong Huang, and Daijun Wei. Route selection for dangerous goods based on d numbers. In *Control and Decision Conference (CCDC), 2016 Chinese*, pages 6651–6656. IEEE, 2016.

[31] Wenbo Wang, Dinh Thai Hoang, Zehui Xiong, Dusit Niyato, Ping Wang, Peizhao Hu, and Yonggang Wen. A survey on consensus mechanisms and mining management in blockchain networks. *arXiv preprint arXiv:1805.02707*, 2018.

[32] Xiwei Xu, Ingo Weber, Mark Staples, Liming Zhu, Jan Bosch, Len Bass, Cesare Pautasso, and Paul Rimba. A taxonomy of blockchain-based systems for architecture design. In *Software Architecture (ICSA), 2017 IEEE International Conference on*, pages 243–252. IEEE, 2017.

[33] Yuchen Yang, Longfei Wu, Guisheng Yin, Lijie Li, and Hongbin Zhao. A survey on security and privacy issues in internet-of-things. *IEEE Internet of Things Journal*, 4(5):1250–1258, 2017.

[34] Jesse Yli-Huumo, Deokyoon Ko, Sujin Choi, Sooyong Park, and Kari Smolander. Where is current research on blockchain technology?a systematic review. *PloS one*, 11(10):e0163477, 2016.

[35] Zibin Zheng, Shaoan Xie, Hong-Ning Dai, and Huaimin Wang. Blockchain challenges and opportunities: A survey. *Work Pap.–2016*, 2016.

[36] Konstantinos G Zografos and Konstantinos N Androutsopoulos. A decision support system for integrated hazardous materials routing and emergency response decisions. *Transportation Research Part C: Emerging Technologies*, 16(6):684–703, 2008.